2018 IEEE Intelligent Vehicles Symposium (IV)
Changshu, Suzhou, China, June 26-30, 2018

Economic Issues in Bitcoin Mining and Blockchain Research

Rui Qin[1], *Member*, *IEEE*, Yong Yuan[1], *Senior Member*, *IEEE*,
Shuai Wang[2] and Fei-Yue Wang[3], *Fellow*, *IEEE*

***Abstract*— With the development of the blockchain technology, Bitcoin mining has become more and more popular. This paper aims to provide a three-level framework of the economic issues in Bitcoin mining research, from the levels of mining pools, individual miners and blockchain network. We also offer an overview of relevant research efforts in literature. Considering the uncertainty, diversity and complexity of the Bitcoin ecosystems, we propose a novel research framework based on the ACP theory, which can be used to explore the economic issues in the Bitcoin ecosystems. This paper aims to provide a preliminary investigation to the economic issues faced by participants in the Bitcoin ecosystems, and stimulate the attentions and interests of researchers in this field.**

Keywords: blockchain, Bitcoin mining, mining pool, blockchain network, economic issues

I. Introduction

Bitcoin, as a decentralized cryptocurrency and a radically new monetary system created in 2008 [21], allows online payments to be sent directly from one person to another without going through financial intermediaries, but through a publicly verifiable ledger called blockchain [33], [34], [35], [36]. The core of the Bitcoin lies in its decentralized consensus protocols, which require all participants in the blockchain network to agree on a common global ledger of transactions, and thus it can effectively prevent double-spending and other disallowed behavior [24].

Bitcoin mining is a process in which a lot of miners race to solve a challenging cryptographic puzzle with their hashing power or mining power. These miners will compete for the right to create a new block and append it to the blockchain ledger, so as to win the block reward from the blockchain system, and the associated transaction fees from the users as a reward of packaging their transactions into the Bitcoin's public ledger. Bitcoin mining provides an effective way for miners to collect Bitcoins as rewards, through contributing their computational power to solve the cryptographic puzzles in the blockchain network in order to find a new block. It is highly relied on the "proof of work" consensus protocol. Typically, a blockchain contains many blocks, and a block can include multiple transactions. To regulate the flow of Bitcoins, each new block is set to be created in about every ten minutes [2]. Once a miner finds a new block, he/she can receive a fixed block reward (currently 12.5 Bitcoins, and will be halved about every four years), as well as the transaction fees provided in the transactions packaged in the new block.

Since Bitcoin mining needs tremendous computational power, it is difficult for small to medium size miners to find a new block. As a result, miners often cooperate and join together to form a mining pool, and divide the rewards from blocks found by the pool to receive a stable revenue. As such, there are three kinds of participants in Bitcoin mining, i.e., the individual miners, the mining pools and the blockchain network. In this paper, we aims to provide a brief introduction of the economic issues in the Bitcoin ecosystems, and propose a research framework for these issues based on the ACP (Artificial societies + Computational experiments + Parallel systems) approach [28].

The rest of this paper is organized as follows. In Section II, we give a brief introduction of the blockchain-based Bitcoin mining and the relevant economic issues. In Section III, we mainly introduce the strategic behavior faced by the mining pools, and in Section IV, we mainly introduce the issues faced by the individual miners. Issues in the blockchain network are introduced in Section V, and in Section VI, we propose a novel research framework based on the ACP approach to study these issues. Section VII concludes our paper.

II. Economic Issues in Bitcoin Ecosystems

A. Bitcoin Mining

The Bitcoin mining processes is given in Fig. 1, and can be described as follows:

(1) The miners of each pool contribute their computational power to the pool in order to solve the

*This work is partially supported by the National Natural Science Foundation of China (71702182, 71472174, 61533019, 71232006) and the Early Career Development Award of SKLMCCS (Y6S9011F4E, Y6S9011F4H, Y6S9011F52).

[1]Rui Qin and Yong Yuan are with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. They are also with Qingdao Academy of Intelligent Industries, Qingdao, China and Beijing Engineering Research Center of Intelligent Systems and Technology, Institute of Automation, Chinese Academy of Sciences, Beijing, China. rui.qin@ia.ac.cn, yong.yuan@ia.ac.cn (Corresponding author)

[2]Shuai Wang is with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. He is also with University of Chinese Academy of Sciences, Beijing, China. wangshuai2015@ia.ac.cn

[3]Fei-Yue Wang is with the State Key Laboratory for Management and Control of Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China. He is also with Qingdao Academy of Intelligent Industries, Qingdao, China and Research Center of Military Computational Experiments and Parallel Systems, National University of Defense Technology, Changsha, China. feiyue.wang@ia.ac.cn

cryptographic puzzle, and submit their shares to the pool as their proof-of-work.

(2) When the pool receives the shares submitted by its miners, it will check if the share is a complete solution. If there is a complete solution, the pool finds a new block, and broadcasts it to all the miners on the blockchain network.

(3) If the new block is confirmed by the blockchain network, the wining pool will win the reward of the block, as well as the transaction fees from the transactions recorded in the block.

(4) The winning pool will distribute the reward as well as the transaction fees among its miners according to their contributions.

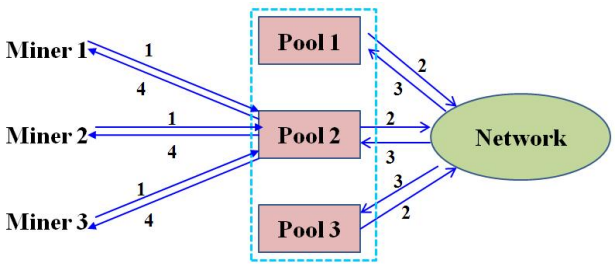

Fig. 1. The process of Bitcoin mining in the blockchain network

B. Framework of Economic Issues

According to the process of Bictoin mining shown in Fig. 1, the economic issues faced by the participants (e.g., miners, pools and blockchain network) of the Bitcoin ecosystems are listed in Fig. 2, from three levels including the individual level, platform level and the market level.

	Miner	Pool	Blockchain Network
Market level		• Mining Game • Selfish Mining	•Bitcoin Transaction Fee
Platform level	• Pool selection • Power Splitting • Pool-hopping	• Reward Mechanism • Incentive Compatibility	
Individual level	•Withholding Attack		

Fig. 2. The economic issues in the Bitcoin mining

In fact, these issues are not isolated, but closely related to each other, and the indepth research on these issues are of great importance to the stability and sustainable developments of the Bitcoin ecosystems. Thus, in the following sections, we will give a detailed introduction for each issue, from the levels of the mining pools, individual miners and blockchain network.

III. Mining Pool

A. Reward Mechanism and Incentive Compatibility of Bitcoin Mining

The mining reward mechanism and its incentive compatibility play an important role in the Bitcoin ecosystems. Now there are many feasible reward mechanisms. If the mechanism is not incentive compatible, it will result in strategic behaviors of the miners, with the purpose of increasing their revenues via gaming the systems. In Bitcoin mining, the reward distribution mechanisms have great importance for miners and pools, since different mechanisms can bring different revenues for them. As stated by Rosenfeld [23], there are many reward distribution mechanisms for mining pools,including simple reward methods such as proportional and pay-per-share (PPS), score-based methods such as Slushes method, Geometric method and pay-per-last-N-shares (PPLNS), and so on. Among these mechanisms, proportional, PPS and PPLNS are three mechanisms commonly used by pools in practice.

- **Proportional**: The proportional reward method is the simplest way for mining pools to distribute the rewards among their miners, where the rewards are distributed among the miners at the end of every round, considering the proportion of the number of shares they submitted to the pool during this round.
- **PPS**: In PPS pools, when a miner submits a share to the pool, he/she can get the expected reward of one share immediately, no matter how many blocks will be found by the pool. In this case, the individual variance of the miners can be greatly reduced, but the pool has a great risk of bankruptcy due to the randomness of the mining process. Traditionally, the pools usually charge a higher service fee from the miners, to compensate such risk.
- **PPLNS**: Unlike the proportional reward method distributing the reward at the end of each round, PPLNS discards the concept of "rounds", and distributes the reward to the miners who submitted shares to the pool more recently, according to the proportions of their submitted shares in the last N shares.

For these reward functions, the properties of incentive compatibility is of great importance for the stability of the pools. Schrijvers et al. [24] proposed a game-theoretic model for reward functions considering a single Bitcoin mining pool, and provided a condition for judgment of the incentive compatibility of a reward. They also showed that under such conditions, the proportional reward function is not incentive compatible, and the PPLNS reward is incentive compatible. Zolotavkin et al. [37] also studied the incentive compatibility of the PPLNS reward, and proposed a general game theoretical model of delays in PPLNS to deal with the issues that miners may increase their revenues by delaying reports of their found shares. They also discussed the conditions for

incentive compatible rewards, and proposed an algorithm to find the Nash equilibria.

B. Mining Game

The process of Bitcoin mining can be regarded as a competing game among all the miners in the Bitcoin ecosystems. If there are multiple valid blocks, only the first be confirmed one can get the reward of the block, and all the other blocks will be discarded [19]. As such, the miners should propagate the new block as quickly as they can. On the other hand, when a miner find a block, he/she can choose any transactions in the memory pool of the blockchain network to be included in the block. However, including more transactions in the block will make the block larger, and take a longer spread time to the Bitcoin network reaching consensus. If he/she is outraced by another miner, the block will become orphaned and the miner can not get any rewards. Thus, the winning probability of the miner might be lowered by including more transactions. Thus, miners face a mining game to get the optimal revenues.

In recent years, the mining game has attracted much attention from researchers in this field. Houy [11] modeled the Bitcoin mining game, and studied its equilibria in the case of two miners. Kiayias et al. [15] established a stochastic game considering the strategic considerations of the miners, and studied two forms of the game with complete information. They showed that a miner with small computational power will follow the expected behavior of the Bitcoin designer, but a miner with large computational power will deviate from the expected behavior. Beccuti & Jaag [1] modeled the mining game as a sequential game with imperfect information, in which miners have to choose whether or not to report their success, and showed that the game has a multiplicity of equilibria. Due to the dynamics of the Bitcoin systems, it is difficulty to predict how long it will take for a miner to find a new block. Lewenberg et al. [16] studied the dynamics of pooled mining and the rewards sharing mechanisms of the pools with cooperative game theoretic tools, and showed that it is difficult for the pools to distribute the rewards among their miners in a stable way.

C. Selfish Mining

The Bitcoin protocol has been proved to be not incentive-compatible due to the existence of selfish mining. For a honest pool, it will broadcast the new block immediately once finding it. However, a minority of pools may keep their discovered blocks private to intentionally fork the chain. Such strategy is called "selfish mining", and it can get more revenues for the selfish pools compared with their ratio of the total mining power by wasting the computational power of the honest nodes.

The concept of selfish mining was first proposed by Eyal & Sirer [8], and the existence of selfish mining made the protocol not incentive-compatible for miners, since colluding miners can obtain a revenue larger than their fair shares, and thus rational miners will prefer to join the selfish miners. Under such conditions, the colluding group will increase in size until it becomes a majority. To solve such problems, a modification to the Bitcoin protocol was proposed, which can protect against selfish mining pools that command less than $1/4$ of the resources. Sapirshtein et al. [26] extended the model proposed by Eyal & Sirer [8], and provided an algorithm to find ε-optimal policies for attackers and the tight upper bounds on the revenue of optimal policies. Elkington [7] used three approaches to analyze selfish mining strategies in the Bitcoin network in order to determine when this strategy will dominate. Solat & Potop-Butucaru [25] proposed a solution for selfish mining, named ZeroBlock, which can prevent block withholding using a technique free of forgeable timestamps, and showed that it is also compliant with nodes churn. Heilman [12] introduced a defense against selfish mining by raising the threshold of mining power necessary to profitably selfishly mine from 25% to 32% under all propagation advantages with the help of unforgeable timestamps.

IV. Miners

A. Pool Selection and Power Splitting

Block mining is a process of solving cryptographic puzzles by calculating hashes, through which a reward can be obtained if a valid block can be found. Block mining needs a great amount of computational resources since finding a block needs to compute a lot of SHA-256 hashes. Generally, a new block can be created every ten minutes in expectation.

Solo mining is a process of mining the block individually, and if the valid block was found, the corresponding miner will be paid the entire reward. Due to the computational difficulty in block mining, solo mining can bring great revenue risks for miners since the variance of solo mining is substantial, and no reward will be obtained until he/she can find a block. Generally, a participant with respectable hardware will need a very long time to find a valid block. As indicated by Lewenberg et al. [16], 687 days in expectation are needed for a miner with a state-of-the-art mining machine to mine a single block. Moreover, due to the randomness and memoryless of the mining process, as well as the ever-increasing popularity of Bitcoin mining, the difficulty is expected to continue to increase, which will increase the variance for miners of solo mining, since miners may get no rewards in a long period. Thus, solo mining is not optimal for miners, especially for those with small mining powers, and a stable income stream and a lower variance in rewards are preferred by miners.

As such, most miners choose to join one or more public pools to reduce the variance of payout and for stable payments. A mining pool allows a mount of miners to work

together on the cryptographic puzzles to find a valid block, and split the rewards among all the miners in the pool according to their contributed computational powers.

As there are a fast growing number of cryptocurrencies and public pools, and different cryptocurrencies and pools may adopt different reward mechanisms and thus produce different revenues for miners, how to select the cryptocurrencies, side chains and pools is a very important issue faced by miners. Moreover, due to the mining power of an individual miner is fixed, how to split his/her power across different cryptocurrencies, side chains and pools is also an important issue faced by miners.

Pool selection and power splitting are the first issue faced by miners in mining pools, and these decisions can affect their revenues greatly. Liu et al. [19] studied the dynamics of mining pool selection problem faced by miners in blockchain network, and proposed an evolutionary game model to study the influence of the hash rate and the block propagation delay on the pool selection strategies of miners. Luu et al. [18] studied the computational power splitting game among a set of competing pools faced by miners, and formulated a model to maximize the net reward of the miners.

B. Withholding Attack

In the mining process, every miner in the pool is given block data combined with a nonce to try to find the solution of the block. Since the solution of the block is difficult to find, the pool will adopt a lower difficulty than the whole blockchain network, and let its miners to submit their solutions of the cryptographic puzzle with the lower difficulty. Such solution is called a "share", which is a partial solution of the block, but can be the complete solution of the block with a certain probability. For example, if a complete solution needs 20 prefixal zeros in the resulting SHA-256 Hashes, then any partial solution with at least, say 10, prefixal zeros will be considered as a share. In fact, if the share is not the complete solution, it means nothing to the pool, but a proof-of-work of the miners. The pool encourages its miners to submit as many shares as they can to prove that they are trying their best to find the solutions of the block. When there is a complete solution in the submitted shares, the pool will broadcast it to the whole block network to get the reward of the new block. After that, the winning pool will distribute the reward of the block to its miners according to their shares.

Traditionally, each miner can know if his/her share is a complete solution. As such, a malicious miner can join the pool, but does not submit any share to the pool, aiming to decrease the mining power of the pool, or withhold the complete solution, but only submit the shares which are not complete solutions to the pool, aiming to decrease the winning probability and thus the expected revenues of the pool and the honest miners. Such attack is called block withholding attack [23], which is a common attack faced by honest miners and pools. The purpose of the attackers is to compel the miners in the pool to leave and thus destroy the pool, which can benefit his/her own pool.

Withholding attack is an important strategic behavior faced by miners and pools, which has been studied by many researchers. Bag et al. [2] studied the sponsored block withholding attack, and proposed a strategy that can effectively counter block withholding attack in any mining pool. Courtois & Bahack [3] proposed a new concrete and practical block withholding attack, and showed that it is difficult or even impossible to detect the miner of block withholding attack. Considering distinct pool reward mechanisms, Tosh et al. [27] established a model for the block withholding attack in a blockchain cloud, and verified the proposed model through simulations. Eyal [5] defined and analyzed a game of the pools, where the pools can use some of their participants to infiltrate other pools and perform the block withholding attack. They show that with any number of pools, no-pool-attacks is not a Nash equilibrium, and in the case of two pools, the miner's dilemma is to decide whether or not to attack. Laszka et al. [17] established a game-theoretic model to study the short-term impacts and long-term impacts of block withholding attacks against mining pools, and studied the conditions of peaceful equilibria and one-sided attack equilibria.

C. Pool-hopping

Due to the existence of large amounts of public pools, how to find the best pool is a critical issue faced by the miners. Miners usually want to maximize his/her expected rewards in the mining games, however, different pools have different mining powers and reward mechanisms, thus, miners need to hop among multiple pools, to find which pool is best for him/her. As shown by Lewenberg et al. [16], it is difficult for a pool to distribute the rewards among its miners in a stable way due to the non-linear nature of returns, and any reward allocation mechanism may has an incentive for some miners to leave their current pool and join other pools, aiming to get higher expected rewards. Such issue is called pool-hopping problems, and with the increasing of the number of public pools, such issue becomes more and more important for miners.

Pool-hopping is an important way for miners to increase their revenues, thus, how to find a pool with higher revenues has become an important issue faced by miners. García & Rodrigues [9] and Chávez & da Silva Rodrigues [4] proposed an algorithm for automatic hopping among mining pools in the Bitcoin network, which can help the miners to find the best pool.

V. Blockchain Network

Bitcoin transaction fee is an important factor in the blockchain network. Due to the rule and protocol of

blockchain, the reward from creating a new block will be halved every four years. When all the Bitcoins were created, the block reward to the miners for finding a new block will diminish to zero, and at that time, the miner might have no incentive to keep mining. The transaction fees solves such problem, and the miners can earn their revenues through transaction fees. Thus, the transaction fee can be regarded as an incentive for the miner to add transactions into a block.

In Bitcoin network, anyone can send money to another one, and due to the limitation of the block size, the amount of transactions that can be included in each block is limited. If the buyers and sellers want their transactions be confirmed as soon as possible, they should pay transaction fees for their transactions. Generally, the transaction fees are voluntarily appended to Bitcoin transactions by buyers and sellers. The size and the time of the transaction, as well as the amount of transaction fee are important factors for the transactions be confirmed by the miners. If the buyers and the sellers want their transactions being confirmed quickly, setting a higher transaction fee is always useful.

Considering the importance of the transaction fees in the Bitcoin ecosystems, Easley [6] investigated the evolution of transaction fees in Bitcoin, and built a framework to explain its development and its influence on the dynamics and stability of the Bitcoin blockchain. Houy [11] studied the economics of Bitcoin's transaction fees in a partial equilibrium setting, and showed that a fixed and imposed transaction fee can keep Bitcoin secure enough if the transaction fee is high enough. They also showed that any situation with a fixed transaction fee can be obtained equivalently by setting a maximum block size instead. However, if we let the transaction fee be the result of a decentralized market and have no constraint on the maximum block size, the transaction fee will eventually go to 0 and miners will not have the necessary incentives to keep mining, hence to keep Bitcoin alive [14]. Möser et al. [20] provided an empirical evidence from a historical analysis of agents' revealed behavior concerning their payment of transaction fees, and identified that a state is sustainable only if fees remain negligible. Huang et al. [13] indicated that there is an upward trend for Bitcoin transaction fee in the future.

VI. An ACP-based Framework for Bitcoin Ecosystems

As blockchain based Bitcoin ecosystem is actually a complex socioeconomic system with the characteristics of uncertainty, diversity and complexity, it can hardly be modeled, analyzed, and solved using traditional computational approaches. Wang [28] proposed a computational framework called ACP, which can be regarded as an effective way to deal with the complex socioeconomic issues [31]. Up to now, the ACP theory has been successfully applied in many fields [22], [29], [30], [32], [38].

In this paper, we propose an ACP-based computational framework to study the economic issues in Bitcoin ecosystems, as shown in Fig. 3, in which we will design one or more artificial Bitcoin systems running in parallel with the real Bitcoin system, to interact, analyze, predict and evaluate the real Bitcoin system. In practice, the economic issues mentioned in this paper can be well studied under the proposed ACP-based computational framework.

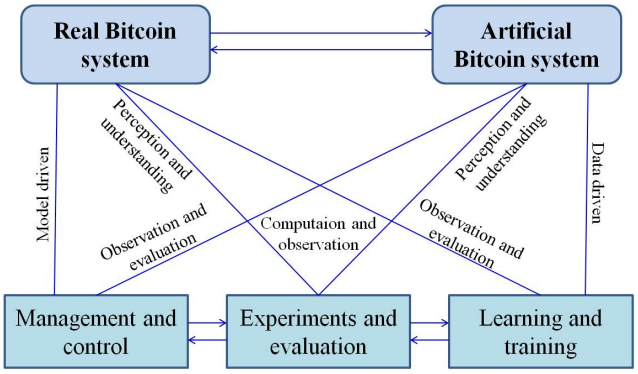

Fig. 3. ACP-based computational framework for Bitcoin ecosystems

As shown in Fig. 3, the parallel Bitcoin system includes three modes of operations [31]. In the experimentation and evaluation operation, we can conduct computational experiments in artificial Bitcoin systems, to analyze and reveal various behaviors and responses of the participants including the miners, pools and blockchain network in the complex Bitcoin ecosystems. Sequentially, we can evaluate various strategies and decisions of the participants and mechanisms of Bitcoin rewards in the artificial Bitcoin systems, to guide the behaviors of the participants in the real Bitcoin system. In the learning and training operation, we will utilize the artificial Bitcoin systems to learn and train the control and management of the complex Bitcoin system, and in the control and management operation, we can utilize the artificial Bitcoin systems to emulate the real Bitcoin system, to improve and optimize the real Bitcoin system's performance in real time with the emerging behaviors of the participants in the artificial Bitcoin systems. Moreover, with the observed feedback from the real Bitcoin systems, we can improve and adjust the parameters of the artificial Bitcoin systems.

VII. Conclusions and Future Work

With the development of blockchain technology and Bitcoin mining, economic issues in blockchain based Bitcoin mining have attracted more and more attention from researchers in the field, and successful and effective solutions for these issues can provide theoretical support for the sustainable development of the blockchain ecosystem. This paper aimed to tease out the economic issues in this field, and present relevant researches in literature on these issues. Moreover, we proposed an ACP based framework to study

the economic issues in Bitcoin ecosystems, aiming to provide important insights for researchers in this field.

This paper gives an overview of the economic issues in the blockchain based Bitcoin systems, and proposed an ACP based framework for studying these issues. In our future work, we will study each of these issues under the framework, and explore their economic insights for the Bitcoin mining and blockchain ecosystems.

REFERENCES

[1] Beccuti, J., Jaag, C. (2017). The Bitcoin mining game: On the optimality of honesty in proof-of-work consensus mechanism, working paper (No. 0060).

[2] Bag, S., Ruj, S., Sakurai, K. (2017). Bitcoin block withholding attack: Analysis and mitigation, IEEE Transactions on Information Forensics and Security, 12(8): 1967–1978.

[3] Courtois, N. T., Bahack, L. (2014). On subversive miner strategies and block withholding attack in Bitcoin digital currency, arXiv preprint arXiv:1402.1718.

[4] Chávez, J. J. G., da Silva Rodrigues, C. K. (2016). Automatic hopping among pools and distributed applications in the Bitcoin network, 2016 XXI Symposium on Signal Processing, Images and Artificial Vision, pp. 1–7, IEEE.

[5] Eyal, I. (2015). The miner's dilemma, 2015 IEEE Symposium on Security and Privacy (SP), San Jose, CA, USA, May 18-20, 2015, pp. 89–103, IEEE.

[6] Easley, D., O'Hara, M., Basu, S. (2017). From mining to markets: The evolution of Bitcoin transaction fees, Social Science Electronic Publishing.

[7] Elkington, J. (2015). Analysis of Selfish Bitcoin Mining Strategies, Social Science Electronic Publishing.

[8] Eyal, I., Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable, International Conference on Financial Cryptography and Data Security, pp. 436–454, March 3-7, 2014, Springer, Berlin, Heidelberg.

[9] García, J. J., Rodrigues, C. K. (2015). A simple algorithm for automatic hopping among pools in Bitcoin mining network, The SIJ Transactions on Computer Networks & Communication Engineering, 3(2): 22–27.

[10] Houy, N. (2014). The economics of Bitcoin transaction fees, Social Science Electronic Publishing.

[11] Houy, N. (2014). The Bitcoin mining game, Working paper GATE 2014-12. 2014.

[12] Heilman, E. (2014). One weird trick to stop selfish miners: Fresh Bitcoins, a solution for the honest miner, International Conference on Financial Cryptography and Data Security, pp. 161–162, March 3-7, 2014, Springer, Berlin, Heidelberg.

[13] Huang, Z.,Li, S., Lu, Y., Wang, Q. (2017). The research on Bitcoin transaction fees based on var model, 7th International Workshop on Computer Science and Engineering (WCSE 2017), pp. 1319–1323, June 25-27, 2017, Beijing, China.

[14] Kaskaloglu, K. (2014). Near zero Bitcoin transaction fees cannot last forever, International Conference on Digital Security and Forensics (DigitalSec2014), pp. 91–99, The Society of Digital Information and Wireless Communication.

[15] Kiayias, A., Koutsoupias, E., Kyropoulou, M., Tselekounis, Y. (2016). Blockchain mining games, 2016 ACM Conference on Economics and Computation, pp. 365–382, July 21, 2016.

[16] Lewenberg, Y., Bachrach, Y., Sompolinsky, Y., Zohar, A., Rosenschein, J. S. (2015). Bitcoin mining pools: A cooperative game theoretic analysis. 2015 International Conference on Autonomous Agents and Multiagent Systems, pp. 919–927.

[17] Laszka, A., Johnson, B., Grossklags, J. (2015). When Bitcoin mining pools run dry: A game-theoretic analysis of the long-term impact of attacks between mining pools, International Conference on Financial Cryptography and Data Security, pp. 63–77, Springer, Berlin, Heidelberg.

[18] Luu, L., Saha, R., Parameshwaran, I., Saxena, P., Hobor, A. (2015, July). On power splitting games in distributed computation: The case of Bitcoin pooled mining, 28th IEEE Computer Security Foundations Symposium, pp. 397–411, IEEE.

[19] Liu, X., Wang, W., Niyato, D., Zhao, N., Wang, P. (2017). Evolutionary game for mining pool selection in blockchain networks, arXiv preprint arXiv:1712.02027.

[20] Möser, M., Böhme, R. (2015). Trends, tips, tolls: A longitudinal study of Bitcoin transaction fees, In International Conference on Financial Cryptography and Data Security, pp. 19–33, Springer Berlin Heidelberg.

[21] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system, Tech. Rep.

[22] Qin, R., Yuan, Y., Wang, F.-Y. (2017). Exploring the optimal granularity for market segmentation in RTB advertising via computational experiment approach, Electronic Commerce Research and Applications, 24: 68–83.

[23] Rosenfeld, M. (2011). Analysis of Bitcoin pooled mining reward systems, arXiv preprint arXiv:1112.4980.

[24] Schrijvers, O., Bonneau, J., Boneh, D., Roughgarden, T. (2016, February). Incentive compatibility of Bitcoin mining pool reward functions, International Conference on Financial Cryptography and Data Security, pp. 477–498, Springer, Berlin, Heidelberg.

[25] Solat, S., Potop-Butucaru, M. (2016). ZeroBlock: Preventing Selfish Mining in Bitcoin, arXiv preprint arXiv:1605.02435.

[26] Sapirshtein, A., Sompolinsky, Y., Zohar, A. (2016). Optimal selfish mining strategies in Bitcoin, International Conference on Financial Cryptography and Data Security, pp. 515–532, Springer, Berlin, Heidelberg.

[27] Tosh, D. K., Shetty, S., Liang, X., Kamhoua, C. A., Kwiat, K. A., Njilla, L. (2017). Security implications of blockchain cloud with analysis of block withholding attack, 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, pp. 458–467, IEEE Press.

[28] Wang, F.-Y. (2004). Artificial societies, computational experiments, and parallel systems: A discussion on computational theory of complex social-economic systems, Complex Systems and Complexity Science, 1(4): 25–35.

[29] Wang, K., Gou, C., Zheng, N., Rehg, J. M., Wang, F.-Y. (2017). Parallel vision for perception and understanding of complex scenes: methods, framework, and perspectives, Artificial Intelligence Review, 48(3): 298–328.

[30] Wang, F.-Y., Xiao, W., Li, L., Li, L. (2016). Step towards parallel intelligence, IEEE/CAA Journal of Automatica Sinica, 3(4): 345–348.

[31] Wen, D., Yuan, Y., Li, X. R. (2013). Artificial societies, computational experiments, and parallel systems: An investigation on a computational theory for complex socioeconomic systems, IEEE Transactions on Services Computing, 6(2): 177–185.

[32] Wang, F.-Y., Zeng, D., Yuan, Y. (2008). An ACP-based Approach for Complexity Analysis of E-commerce System, Complex Systems and Complexity Science, 3: 1–8.

[33] Yuan, Y., Wang, F.-Y. (2016). Blockchain: The state of the art and future trends, Acta Automatica Sinica, 42(4): 481–494.

[34] Yuan, Y., Wang, F.-Y. (2016). Towards Blockchain-based Intelligent Transportation Systems, 19th IEEE International Conference on Intelligent Transportation Systems (ITSC2016), Rio de Janeiro, Brazil, pp. 2663–2668.

[35] Yuan, Y., Wang, F.-Y. (2017). Parallel Blockchain: Concept, Methods and Issues, Acta Automatica Sinica, 43(10): 1703–1712.

[36] Yuan, Y., Zhou, T., Zhou, A.-Y., Duan Y.-C., Wang, F.-Y. (2017) Blockchain technology: From data intelligence to knowledge automation, Acta Automatica Sinica, 43(9): 1485–1490.

[37] Zolotavkin, Y., García, J., Rudolph, C. (2017, October). Incentive Compatibility of Pay Per Last N Shares in Bitcoin Mining Pools, International Conference on Decision and Game Theory for Security, pp. 21–39, Springer, Cham.

[38] Zhang, N., Wang, F.-Y., Zhu, F., et al. (2008). DynaCAS: Computational experiments and decision support for ITS, IEEE Intelligent Systems, 23(6): 19–23.